Summer School on Elliptic and Hyperelliptic Curve Cryptography

Exercises for lectures on Tuesday, 04.09.2007

1. Let p be prime, and let $\mathbb{F}_p$ be the finite field with p elements.
   (a) Let $\alpha, \beta \in \mathbb{F}_p^*$ be non-squares. Prove that the product $\alpha\beta$ is a square.
   (b) Let $E/\mathbb{F}_p$ be the elliptic curve defined by the Weierstrass equation $Y^2 = X^3 + aX + b$, and let $t = p + 1 - \#E(\mathbb{F}_p) \in \mathbb{Z}$. By Hasse's Theorem (see Dan Bernstein's talk) $|t| \leq 2\sqrt{p}$.
   For a non-square $g \in \mathbb{F}_p^*$, define the curve $E_g : Y^2 = X^3 + g^2aX + bg^3$. Prove that E_g has $p+1+t$ points. ('The' curve E_g is called the *quadratic twist* of E.)

2. An elliptic curve E defined over $\mathbb{F}_q, q = p^r$ is supersingular if one of the following equivalent conditions holds
   (a) $E[p^s](\overline{\mathbb{F}}_q) = \{P_\infty\}$ (for $s \in \mathbb{N}$).
   (b) $|E(\mathbb{F}_q)| = q - t + 1$ with $t \equiv 0 \bmod p$.
   (c) End_E is order in quaternion algebra.
   Show that an elliptic curve of the form $y^2 + a_3y = x^3 + a_2x^2 + a_4x + a_6, a_3 \in \mathbb{F}_{2^n}^*, a_2, a_4, a_6 \in \mathbb{F}_{2^n}$ is non-singular. Show that such elliptic curves are supersingular. Hint: use the criterion on the 2-torsion.

3. Consider $C : y^2 = x^5 + 4x^3 + 3x^2 + 11x + 5$ over $\mathbb{F}_{17}$. Find at least one divisor class defined over $\mathbb{F}_{17}$ where in the Mumford representation u is irreducible of degree 2. This is almost Exercise 8 from yesterday, but with the restriction that here u should be irreducible.

4. Show that for $p \equiv 2 \bmod 3$ the curve $E_b/\mathbb{F}_p : y^2 = x^3 + b$ has $|E_b(\mathbb{F}_p)| = p + 1$.
   Thus the embedding degree for this curve is ≤ 2 as any prime r with $r|p+1$ also divides $p^2 - 1 = (p-1)(p+1)$. Verify that there is a *distortion map* $\varphi : E_b(\mathbb{F}_p) \to E_b(\mathbb{F}_{p^2})$ defined by $\varphi(x, y) \mapsto (\xi_3 x, y)$ mapping to $E_b(\mathbb{F}_{p^2}) \setminus E_b(\mathbb{F}_p) \cup \{P_\infty\}$, where ξ_3 is a third root of unity in $\mathbb{F}_{p^2}$.

5. Let $p = 5387$. In that case $\mathbb{F}_p^* = \langle 2 \rangle$ is generated by 2. We want to solve the DLP $h = 2^x$ in $\mathbb{F}_p^*$ using the factor base $\mathcal{F}(11) = \{2, 3, 5, 7, 11\}$. Hints:
   (a) To find relations try arbitrary exponents – or use 2^r for $r \in \{1067, 3721, 4409, 1619, 2072, 4200, 4806\}$.
   (b) Compute the discrete logarithm $x(q)$ for all elements q in the factorbase $q = 2^{x(q)}$. E.g. the exponent 1619 directly gives the discrete logarithm of 7.
   (c) Finally find a power y of 2 so that $h \cdot 2^y$ is B-smooth. If you are desperate, try $y = 145$.

6. The DLP in $\mathrm{Pic}_C^0(\mathbb{F}_{2^n})$ of the genus 9 hyperelliptic curve C given by $C : y^2 + y = x^{19} + x^{17} + x + 1$ should be weak under index calculus attacks.
   Find all divisor classes with irreducible u of degree ≤ 3 defined over $\mathbb{F}_2$.